eSecurity

Treinamentos em Segurança da Informação

O que temos para hoje?

Menu do dia:

- ✓ **SNORT**
  - ✓ Entendendo o Snort
- ✓ **GUARDIAN**
  - ✓ Entendendo o Guardian
- ✓ **Mão na massa**
  - ✓ Material necessário
  - ✓ Instalando SNORT
  - ✓ Configurando SNORT
  - ✓ Instalando Guardian
  - ✓ Configurando Guardian

O Snort

Entendendo o SNORT

Os módulos que compõe o Snort são ferramentas poderosas, capazes de produzir uma grande quantidade de informação sobre os ataques monitorados, dado que é possível avaliar tanto o cabeçalho quanto o conteúdo dos pacotes, além de disponibilizar, por exemplo, a opção de capturar uma sessão inteira.

O Snort monitora o tráfego de pacotes em redes IP, realizando análises em tempo real sobre diversos protocolos (nível de rede e aplicação) e sobre o conteúdo (hexa e ASCII). Outro ponto positivo desse software é o grande número de possibilidades de tratamento dos alertas gerados. O subsistema de registro e alerta é selecionado em tempo de execução através de argumentos na linha de comando, são três opções de registro e cinco de alerta. O registro pode ser configurado para armazenar pacotes decodificados e legíveis em uma estrutura de diretório baseada em IP, ou no formato binário do tcpdump em um único arquivo. Para um incremento de desempenho, o registro pode ser desligado completamente, permanecendo os alertas. Já os alertas podem, ser enviados ao syslog, registrados num arquivo de texto puro em dois formatos diferentes, ou ser enviados como mensagens WinPopup usando o smbclient.

Entendendo o SNORT

Os alertas podem ser enviados para arquivo texto de forma completa e o alerta rápido. O alerta completo escreve a mensagem de alerta associada à regra e a informação do cabeçalho do pacote até o protocolo de camada de transporte. A opção de alerta rápido escreve um subconjunto condensado de informação do cabeçalho alerta.

Por fim, uma última opção desabilita os alertas completamente.Existe também, a possibilidade de utilizar métodos como o Database Plug-in por exemplo, para registrar pacotes em uma variedade de bases de dados diferentes (MySQL, PostgreSQL, entre outros), as quais contam com recursos próprios para efetuar consultas, correlações e dispõem de mecanismos de visualização para analisar dados.

Entendendo o SNORT

O Snort deve trabalhar em todos os lugares que o libpcap trabalha, e o mesmo foi compilado com sucesso nas seguintes plataformas:

I386	Sparc	M68k/PPC	Alpha	Other	
X	X	X	X	X	Linux
X	X	X	-	-	OpenBSD
X	-	-	X	-	FreeBSD
X	-	X	-	-	NetBSD
X	X	-	-	-	Solaris
-	X	-	-	-	SunOS 4.1.x
-	-	-	-	X	HP-UX
-	-	-	-	X	AIX
-	-	-	-	X	IRIX
-	-	-	X	-	Tru64
-	-	X	-	-	MacOS X Server
	-	-	-	-	Win32

Fonte: Viva o Linux

O Guardian

Download more graphics at www.psdgraphics.com

GUARDIAN

Entendendo o Guardian

O Guardian gera automaticamente regras de firewall para bloquear os endereços de origem que estão atacando o nosso servidor.

E ele dá suporte a vários tipos de firewall, ex.: iptables, ipchains, ipfwadm, ipfilter

O "snort" analisa o pacote e da a ele uma pontuação de periculosidade , e o "guardian" estando ligado insere uma regra dinamicamente no firewall; por exemplo, se alguém faz um portscan, o snort percebe e informa para o guardian bloquear aquela origem.

Voce escolhe qual a interface de rede e a rede logica que ele tem que ouvir através da interface web geralmente a externa.

Colocando em prática

Material necessário

Iniciaremos com uma instalação simples do Ubuntu Server, afins de, apresentar a instalação do zero.

Baixe a imagem no link abaixo:
http://releases.ubuntu.com/14.04/ubuntu-14.04.1-server-i386.iso

Caso esse link não venha funcionar algum dia, baixe sempre a ultima versão do ubuntu server neste link:
http://releases.ubuntu.com/

Instalando SNORT

Após a instalação do ubuntu em uma máquina virtual, faça a instalação das seguintes aplicações:

```
apt-get install snort
```

Realiza a instalação do Snort. Ele ficará localizado em /etc/snort
Acesse a pasta /etc/snort

```
mv snort.conf  snort.conf.orig
```

Cria uma cópia de segurança das configurações padrão do Snort

```
cat snort.conf.orig |grep –v ^# |grep . > snort.conf
```

Cria um cópia do arquivo de configuração e remove todas as linhas que possuem
Edite o arquivo snort.conf e coloque o IP principal do seu NIDS na variável HOME_NET
Na ultima linha, adicione o destino do arquivo de alerta: output alert_full: /var/log/snort/alert

Instalando SNORT

/etc/init.d/snort start
Inicia o Serviço do Snort

/etc/init.d/snort stop
Para o serviço do Snort

Snort –v
Apresenta os pacotes capturados pelo snort realtime

Snort –vd
Apresenta os pacotes e dados capturados pelo snort realtime

tail –f /var/log/snort/alert
Monitora em tempo real os alertas gerados pelo SNORT

Instalando Guardian

O guardian é um conjuto de scripts, desenvolvido em Perl.
É importante mantê-los exatamente nas pastas citadas abaixo:

```
wget –cv  http://www.chaotic.org/guardian/guardian-1.7.tar.gz
tar –xvzf guardian-1.7.tar.gz
cd guardian-1.7
```

Acesse o arquivo de configuração e coloque os seguintes dados

```
vi guardian.conf
HostIpAddr                192.168.2.11 #IP DO SNORT
Interface                 eth0
AlertFile                  /var/log/snort/alert
TargetFile                 /etc/guardian.target
```

Copie a configuração do guardian para a pasta /etc

```
cp guardian.conf /etc/
```

Instalando Guardian


```
# Adicione o IP do NIDS na lista de máquinas que não serão bloqueadas
echo 192.168.2.11 > /etc/guardian.ignore

# Adicione o IP do NIDS na lista de máquinas que podem ser alvos
echo 192.168.2.11 > /etc/guardian.target

# Copie os scripts para as patas corretas
cd scripts
cp iptables_block.sh /sbin/guardian_block.sh
cp iptables_unblock.sh /sbin/guardian_unblock.sh
cd /opt/guardian-1.7
cp guardian.pl /sbin
touch  /var/log/guardian.log
```

Instalando Guardian

\# Crie o script de inicialização automatizada do Guardian

vi /etc/init.d/guardian

```
#!/bin/bash
test -f /sbin/guardian.pl || exit 0
case "$1" in
        start)
          guardian.pl -c /etc/guardian.conf
          ;;
        stop)
          kill -9 $(pgrep guardian.pl)
          ;;
        *)
          echo "Opção invalida. Use start ou stop."
          exit 2
          ;;
esac
exit 0
```

\# Dê permissão 775 para o script que você acabou de criar

Chega por hoje

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Skype: desafiohacker

Fanpage: www.facebook.com/academiahacker